



Joomla 5.4.9 and 6.1.4 Fix 16 Security Issues, Two Rated High

Joomla 5.4.9 and 6.1.4 fix 16 core security issues, including cache directory deletion, SSRF, an MFA bypass and account creation with registration switched off.

Phil E. Taylor | 29 September 2026

The Joomla project released [Joomla 5.4.9 and 6.1.4](#) on 29 September 2026, and both fix the same sixteen core security issues, CVE-2026-90906 to CVE-2026-92232. Two are rated High by the Joomla Security Strike Team: a cache purge that can delete any directory the web server can write to, and server-side request forgery through URL fields in several core extensions. The rest are seven cross-site scripting fixes, six access control fixes and an MFA bypass through Remember Me cookies.

The advisories give a title, a severity and a version range, and not much else. We read the code behind each one to find out who can actually reach it, because that decides the order you patch in far more than the severity label does. The two High issues both need a backend login. One of the Moderate ones needs nothing at all.

What to do now

Update Joomla 5 sites to 5.4.9 and Joomla 6 sites to 6.1.4. Joomla 4 sites must go to 4.4 before 5.4.9, and 5.x sites must be on 5.4 before 6.1.4. Five of these flaws reach back to Joomla 1.5 or 3.0, and Joomla 3 gets no fix from the Joomla project. The 6.2.0 betas did not have the fixes at release time.

TL;DR

- **16 core fixes** in one release, all credited to outside researchers, none to us
- **High:** arbitrary directory deletion through System, Clear Cache (CVE-2026-90915) and SSRF through feed and request URLs (CVE-2026-92222). Both need a backend account
- **Reachable anonymously on every site:** CVE-2026-90907 lets a visitor create a Guest account with registration switched off, back to Joomla 1.5
- **MFA bypass** (CVE-2026-92227) needs the password, then uses a Remember Me cookie to skip the second factor on later front-end logins

- **Five issues reach Joomla 3**, where about one in four of the Joomla sites in the mySites.guru database still run
- The **Template Manager bug** from 5.4.8 and 6.1.3 is fixed in this release too
- **Known issue on 5.4.9**: editing items through the Joomla API fails with a fatal error. A one-line workaround is below, and 6.1.4 is not affected

All Sixteen Joomla Security Issues in One Table

The Joomla Security Centre published [all sixteen advisories](#) about an hour after the release. Every one is fixed in 5.4.9 and 6.1.4. The "Who can reach it" column is our reading of the code, not something the advisories state, and it assumes Joomla's default permissions.

CVE	Severity	Issue	Affected from	Who can reach it	Reported
CVE-2026-90915	High	Arbitrary directory deletion via cache purge	4.0.0	Administrator	Aria Akhavan
CVE-2026-92222	High	SSRF in several core extensions	3.0.0	Manager and up	Aria Akhavan
CVE-2026-90907	Moderate	Account creation via profile.save	1.5.0	Anyone	Adithyan
CVE-2026-92227	Moderate	MFA bypass through Remember Me cookies	4.0.0	Password holder	Google ai Ada Logic Mukul Go
CVE-2026-90917	Moderate	Tagged items shown from restricted categories	4.0.0	Anyone	Sabuhi Mammad

CVE	Severity	Issue	Affected from	Who can reach it	Reported
<u>CVE-2026-90918</u>	Moderate	XSS in HTML mail templates	4.0.0	Anyone, if HTML mail is on	Joe Grey
<u>CVE-2026-92231</u>	Moderate	InputFilter bypass via HTML5 entities	1.5.0	Filtered content authors	Netanel Stern
<u>CVE-2026-92232</u>	Moderate	InputFilter bypass via whitespace in data URIs	1.5.0	Filtered content authors	not stated
<u>CVE-2026-90906</u>	Moderate	XSS in <code>HTMLHelper::link</code>	1.5.0	Depends on the caller	Demyanc V.
<u>CVE-2026-90914</u>	Moderate	XSS in audio and video layouts	4.0.0	Content editors	Aria Akhavan
<u>CVE-2026-92224</u>	Moderate	XSS in link toolbar layout	4.0.0	Depends on the caller	Google ai Ada Logic
<u>CVE-2026-92225</u>	Moderate	XSS in the module list	4.0.0	Module editors	Google ai Ada Logic
<u>CVE-2026-92223</u>	Moderate	Workflow stage change without permission	5.0.0	Backend editors, if Workflows are on	Faceless
<u>CVE-2026-90913</u>	Moderate	Access level changes through the API	4.0.0	API users below Super User	sec-reex
<u>CVE-2026-92226</u>	Moderate	API edits ignoring item permissions	4.0.0	API users below Super User	Google ai Ada Logic

CVE	Severity	Issue	Affected from	Who can reach it	Reported
<u>CVE-2026-90916</u>	Low	Content history compare shows other items	4.0.0	Anyone who edits content	Arkadiusz

The CVE records themselves had not been published at cve.org when this was written, so the advisories are the authoritative source for now.

Patching Joomla 5.4.9 and 6.1.4 Across a Client Portfolio

On one site this is a single click. Across a portfolio, the first job is working out which sites need which path, and the numbers from the Joomla sites in the mySites.guru database, taken minutes after the release, show where the work is.

73.1%

of Joomla sites run a version this release fixes

every 4.x, 5.x below 5.4.9, 6.x below 6.1.4

26.0%

are on Joomla 3

five of the sixteen flaws reach them, with no fix

90.6%

of Joomla 5 and 6 sites reached the previous release

six weeks after 5.4.8 and 6.1.3 shipped

Joomla sites in the mySites.guru database that reported in during the 30 days to 29 September 2026.

That last figure is the encouraging one. Nine in ten Joomla 5 and 6 sites in the mySites.guru database were on the latest release six weeks after it came out, so most people managing them do update. The remaining one in ten is where incidents come from, and those sites are rarely left behind on purpose: the site on a different host, the

one whose update stalled during download, the client who has their own admin login and clicked “later”.

mySites.guru’s Joomla version check flags each connected site behind the latest release in its branch, so all your 5.4.8 and 6.1.3 sites are now flagged. You can [manage multiple Joomla sites](#) from that one list and run the core update on all of them in one pass. The guide on [mass upgrading Joomla and WordPress sites from one dashboard](#) shows the click path, and the opt-in [update queue](#) runs one update at a time per server so a shared host is not hit by thirty at once.

Joomla CMS Version Must Be Up-to-date

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

Some sites will update themselves. Joomla 5.4 and later can take [automated core updates](#) from the Joomla project’s own free update service, which is on by default for new 5.4 and 6.x installs and off for sites upgraded from older versions. That is a Joomla feature rather than a mySites.guru one, and a site where it is off, or which cannot reach the update server, stays where it is. Check the version each site actually reports rather than assuming.

Two upgrade-path rules from the release notes catch people out. Joomla 5.4.9 needs 4.4 as its starting point, so a Joomla 4.3 site goes to 4.4 first. Joomla 6.1.4 needs 5.4, so a 5.3 site goes to 5.4.9 before it goes anywhere near 6. Both releases also add one database column (`#__updates.security` , explained below), so take a backup first. A site that fails at the database step is much easier to put back from a backup than to repair.

The Joomla Flaw That Reaches Every Site: Account Creation With Registration Off

We would patch for [CVE-2026-90907](#), first, ahead of both High issues. It is rated Moderate, but it needs no login and no special configuration, and it reaches back to Joomla 1.5.

The front-end profile form saves through a `profile.save` task in `com_users`. Before this release, that task checked the form token and nothing else. A visitor who was not logged in has a user id of zero, so the save ran against a new, empty user: Joomla bound the posted name, username, email and password, put the account in the configured guest group (Guest, by default), and saved it. The Allow User Registration setting is never consulted on that path. The fix is three lines in

`ProfileController::save()` that refuse the request if the user is a guest.

On a default site, what an attacker gets is limited:

- The account is in the Guest group, which has no front-end login permission by default, so it cannot sign in
- It is not blocked, and the attacker chose its password, so it becomes a working login the moment someone grants Guest more rights or points the guest group somewhere else
- It exists. It can hold an email address or username so the real person cannot register with it
- User plugins run for it. A CRM sync, a newsletter auto-subscribe or a community profile plugin that acts on `onUserAfterSave` fires for every account created this way

The practical clean-up is to sort Users by registration date on sites where registration is switched off and look at anything in the Guest group you do not recognise.

mySites.guru's [user registration check](#) tells you which sites have registration on, and [managing users across every site](#) makes the review a single search rather than an admin login per site. For accounts with real rights, the [rogue administrator detection](#) is the check to run.

The Two High-Severity Joomla Issues

Both High issues need a backend account, which is why the JSST rates their probability Low. The impact is what earns them High.

Deleting directories through the cache purge (CVE-2026-90915)

System, Clear Cache sends the names of the cache groups to delete, and the file cache handler joined each name onto the cache folder path and deleted the result. Its safety check only confirmed the path *started* with the cache folder. It never resolved `..`, so a group name like `../../images` passed the check and deleted the images folder, and so on up to anything the web server user can write to.

The request has a CSRF token, so it cannot be triggered by a link. The people who can send it are those with access to Clear Cache, which by default is the Administrator and Super User groups. The concern is an Administrator, or anyone a site builder has given cache access, being able to destroy the whole site's files, which is far beyond what that role should allow. It only applies with the file cache handler, which is Joomla's default. The fix routes every cache path through `Path::check()`, which resolves the path and refuses anything outside the cache folder.

Server-side request forgery through URL fields (CVE-2026-92222)

Joomla's URL validation rule accepts over twenty schemes when a form field does not name its own list: `file`, `gopher`, `ldap`, `ftp` and more alongside `http` and `https`. Most URL fields only store a link, but four make the server fetch whatever URL they hold:

- **News Feeds items**, reachable by Manager and up, the lowest-privileged route
- **The Feed Display module**, site and administrator versions, reachable by anyone who can create modules
- **The scheduled GET Request task**, which also writes the response into the task output, so whoever set it up can read what came back
- **The custom update source** in Joomla Update, Super User only

The fix limits those fields to `http` and `https` (plus `ftp` and `ftps` for the update source). Our reading of the feed code is that it opened the URL with PHP's `XMLReader` before anything else, which would also make local XML files readable through `file://`; the advisory does not go into that detail. This one reaches back to Joomla 3.0.0, and the Regular Labs Modules Anywhere fix two days earlier used the same Feed module as its route to the server's files.

The Joomla MFA Bypass Through Remember Me

CVE-2026-92227 is the fourth MFA bypass Joomla has fixed this year, and it needs the password first. Joomla issued the Remember Me cookie the moment the password was accepted, before the MFA prompt appeared. By default, Joomla also skips MFA for logins made by cookie. Put together, someone with a user's password could tick Remember Me, abandon the MFA screen, and return later in a fresh browser session to be logged in by the cookie without ever entering a second factor.

The fix holds the cookie back until MFA has been passed. It affects front-end logins only, because the administrator login has no Remember Me, and both plugins involved (Authentication - Cookie and System - Remember Me) are enabled by default. The same release also switches the TOTP code comparison to `hash_equals()` (#48056), so variants like `+123456` no longer pass for the real code.

If you are forcing MFA on Super Users across a portfolio, patch first. That post also explains why cookie logins skip MFA by default and how to change that setting, which is sensible with or without this fix.

Force Multi-Factor Authentication For Super Users

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

The Joomla Cross-Site Scripting Fixes

Seven of the sixteen are cross-site scripting, where a value ends up in a page or email without being escaped. How much each one matters depends almost entirely on who can supply the value:

- **InputFilter, two bypasses** (CVE-2026-92231, CVE-2026-92232). This is the filter that cleans HTML from users who are not on No Filtering, which by default includes Authors and Editors. One bypass hid `javascript:` behind HTML5 entities such as `
`; the other hid a `data:text/html` link behind a tab character that browsers drop. Both date back to 1.5.0 and follow the two InputFilter fixes in [5.4.6](#) and [6.1.1](#). If you let people you do not fully trust write content, these are the XSS fixes that matter
- **HTML mail templates** (CVE-2026-90918). Joomla already marked values like the contact form's name and message as unsafe, but on sites sending HTML mail they were inserted raw anyway. Visitors could put markup into mail sent to the site owner. The default is plain text, so most sites were not exposed
- **Audio and video output** (CVE-2026-90914). Only the `src` attribute of the media field's audio and video output was escaped. The advisory's range starts at 4.0.0, but the layouts it fixes only exist on Joomla 6, and 5.4.9 changes nothing for it
- **The module list** (CVE-2026-92225). A module position string was printed unescaped into the backend Modules list, so someone who can edit modules could plant script for a Super User who opens the list
- **HTMLHelper::link** and the link toolbar (CVE-2026-90906, CVE-2026-92224). Library helpers that printed URLs unescaped. Whether a site is exploitable depends on some caller, core or third-party, passing a user-influenced URL to them, which is why both are rated Low probability

The Joomla Access Control Fixes

The other six are places where Joomla checked the wrong permission, or checked one and forgot another:

- **Tagged items** (CVE-2026-90917). Tag lists, Popular Tags and Similar Tags checked an article's own access level but not its category's. An article left Public inside a Registered-only category showed up for anonymous visitors
- **Content history compare** (CVE-2026-90916, Low). The compare view checked the first version id and not the second, so anyone who can edit one item with history could read old versions of items they cannot open
- **Workflow stage changes** (CVE-2026-92223). The batch stage change set an error when the user lacked permission and then made the change anyway. Workflows are off by default, so only sites that turned them on for Joomla 5 and 6 publishing workflows are affected
- **The Joomla API** (CVE-2026-90913, CVE-2026-92226). API users could create and edit viewing access levels with ordinary user-management rights where the backend requires full admin, and API edits ignored item-level permissions. By default only Super Users can log in to the API, so these matter on sites that have given API access to a lower group for an integration

If nothing on a site uses the API, switching the Joomla API off removes that whole class of problem, and the API tokens you have issued are worth a review whether or not you do.

Disable The Joomla API (Web Services)

mySites.guru checks every connected site for this automatically and flags it the moment it appears. It runs as part of the full audit on every connected site.

Check your site for free →

Joomla 3 Sites Get No Fix

Five of the sixteen reach back to Joomla 1.5.0 or 3.0.0: the anonymous account creation, the SSRF, both InputFilter bypasses and the `HTMLHelper::link` escaping. Joomla 3 has been end of life since August 2023, so the Joomla project will not patch any of them there.

In the mySites.guru database, 26.0% of Joomla sites that reported in over the last 30 days are still on Joomla 3, roughly one in four. Each of them now has a publicly documented way for an anonymous visitor to create accounts, with the exact file and the three missing lines named in a public diff. The [Joomla 3 end-of-life check](#) lists those sites, and [what Joomla 3 end of life means for agency retainers](#) covers the options for them.

An unsupported CMS collects known flaws

Each Joomla release like this one adds to the list of documented, unfixed problems on every Joomla 3 site. Nothing about those sites changed today, yet they are less safe than they were yesterday.

Known Issue: Joomla 5.4.9 Breaks API Edits

A few hours after the release, Joomla published a [known issues page for 5.4.9](#). Updating an item through the Joomla API, with a PATCH request to change a banner, a user or an article, now stops with a fatal error.

The cause is the new item permission check in `ApiController::allowEdit()`, part of the fix for API edits ignoring item permissions. It calls `InflectorFactory`, but the `use` statement that imports the class was lost when the fixes were ported to the 5.x branch, so PHP cannot find it. The 6.1.4 copy of the file has the import, which is why only 5.4.9 is affected. The fix is [#48527](#), merged the same evening and due in 5.4.10.

If an integration writes to a 5.4.9 site through the API, add this line with the other `use` statements near the top of `libraries/src/MVC/Controller/ApiController.php` :

```
use Doctrine\Inflector\InflectorFactory;
```

That is exactly what #48527 adds, so 5.4.10 will overwrite the file with the same fix. Reading items through the API still works, and a site where nothing uses the API never touches this code, so neither is a reason to hold back 5.4.9 and its sixteen security fixes. If the API on a site is switched on but nothing uses it, this is a good moment to switch it off.

Other Changes in Joomla 5.4.9 and 6.1.4

The Template Manager is fixed

The Template Manager bug that 5.4.8 and 6.1.3 introduced, where creating an override or a new template folder failed with "Snooping out of bounds", is fixed in both releases by #48274. Two other Template Manager fixes in the same release also changed `TemplateModel.php`, so the file that ships is not identical to the replacement Joomla published as a known issue, or to the one our fix tool installed. The update overwrites either, which is what you want.

Extensions can now mark a security release

#48233 lets an extension's update feed flag an update with a `<security>` level from 0 (None) to 4 (Critical). Joomla stores the highest level among all updates newer than the installed version in the new `#__updates.security` column, and System, Update, Extensions shows a "Security release level" badge. That is the database change in this release. It only helps once extension developers start sending the flag, but it is the first time core Joomla has had a way to tell you an extension update is a security fix rather than a feature release.

Smaller changes in this release

- **POWCaptcha** no longer uses a CSRF token for its challenge on 6.1 ([#48304](#)), because page caching served one visitor's token to the next and broke the captcha
- **Banner tracks CSV export** escapes names that start with `=`, `+`, `-` or `@` ([#48047](#)), closing a spreadsheet formula injection
- **Tagged articles** stop creating a duplicate `#__ucm_content` row on every save ([#48221](#))
- **Bundled libraries:** `joomla/filter` is updated for the InputFilter fixes, `joomla/filesystem` moves to a public release containing the SHTML upload fix from 5.4.8, and `joomla/registry` and `paragonie/sodium_compat` get point releases

Joomla 6.2 beta sites

The 6.2.0 betas and the 6.2 development branch did not have these fixes when 5.4.9 and 6.1.4 shipped. If you run a 6.2 beta anywhere public, it is exposed until the next beta.

What We Would Do Tonight

1. Patch sites with front-end logins, MFA users, restricted categories or HTML mail first. Those are the sites where an anonymous visitor or a stolen password can reach something
2. Patch everything else on Joomla 4, 5 and 6 in one bulk run
3. Check each site reports 5.4.9 or 6.1.4 from its own files, and chase the ones that did not move
4. On 5.4.9 sites where an integration edits content through the API, apply the [one-line workaround](#) until 5.4.10
5. On sites with registration off, look for Guest accounts created before the update
6. Put a date on the Joomla 3 sites. They will not get this fix or the next one

Previous releases in this series: [5.4.6 and 6.1.1](#) fixed ten issues including two MFA bypasses, and [5.4.7 and 6.1.2](#) shipped the regression that ignored article options. If you are not yet managing your Joomla sites from one place, the [free audit](#) runs the version check on your own sites, and [pricing](#) covers everything else the subscription does.

Timeline

-
- A vertical timeline with a central line and circular markers. The markers are open circles for reports and releases, and filled circles for advisories and API issues. The dates are listed on the left, and the descriptions are on the right.
- 2026-07-15** ○ **The earliest of the sixteen reports reaches the JSST**
The content history comparison view issue, CVE-2026-90916. The rest arrive between late July and 10 September.
 - 2026-09-10** ○ **Google and Ada Logics report four issues in one day**
The link toolbar and module list XSS, the webservice edit check and, jointly with Mukul Goyal, the Remember Me MFA bypass.
 - 2026-09-17** ○ **Release candidates ship without the security fixes**
5.4.9-rc1 and 6.1.4-rc1 contain only the public bug fixes. The security changes went into the final release commits.
 - 2026-09-29** ● **Joomla 5.4.9 and 6.1.4 are released**
Both at 16:00 UTC, each described as a security release to install as soon as possible.
 - 2026-09-29** ● **All sixteen advisories go up on the Security Centre**
About an hour after the release, with CVE ids, version ranges and credits.
 - 2026-09-29** ● **API edits found broken on 5.4.9**
About an hour after the release, pull request #48527 is opened: a use statement lost while porting the security fixes to 5.x makes every API PATCH request fatal. 6.1.4 is not affected.

2026-09-29



Joomla publishes the 5.4.9 known issue

The known issues page goes up at 19:07 UTC with a one-line workaround for `libraries/src/MVC/Controller/ApiController.php`.

2026-09-29



The fix is merged for 5.4.10

#48527 is merged into the 5.4 branch at 19:36 UTC. It adds the same line as the workaround, so 5.4.10 overwrites a patched file with identical code.

Further Reading

- [Joomla 5.4.9 Known Issues](#) - the API edit regression and its one-line workaround.
- [Joomla 6.1.4 and 5.4.9 Security and Bugfix Release](#) - the joomla.org announcement, with the full list of bug fixes.
- [Joomla Security Centre](#) - all sixteen advisories, with version ranges and credits.
- [GitHub release notes for 5.4.9](#) and [6.1.4](#) - packages, checksums and the upgrade-path notes.
- [5.4.8 to 5.4.9](#) and [6.1.3 to 6.1.4](#) - every changed file in each release.

To see which of your Joomla sites are still behind 5.4.9 or 6.1.4, run a [free audit](#). No credit card needed.

Frequently Asked Questions

Does Joomla 5.4.9 break the Joomla API?

Editing an item through the API does. On 5.4.9, a PATCH request to update a banner, a user or any other item stops with a fatal error, because a use statement for InflectorFactory went missing when the security fixes were ported to the 5.x branch. Joomla lists it as a known issue, and the fix, pull request #48527, was merged on 29 September 2026 for 5.4.10. Until then, add use Doctrine\Inflector\InflectorFactory; to the use statements at the top of libraries/src/MVC/Controller/ApiController.php. Joomla 6.1.4 is not affected, and nor is any site that does not use the API.

What is fixed in Joomla 5.4.9 and 6.1.4?

Sixteen core security issues, CVE-2026-90906 to CVE-2026-92232. Two are rated High: arbitrary directory deletion through the cache purge action, and server-side request forgery through URL fields in several core extensions. The other fourteen are seven cross-site scripting fixes, six access control fixes and one MFA bypass, all rated Moderate except one Low.

Which Joomla versions are affected?

Every 4.x, every 5.x up to 5.4.8 and every 6.x up to 6.1.3. Five of the sixteen issues reach further back, to Joomla 1.5.0 or 3.0.0, which means Joomla 3 sites are affected and will not get an official fix. The 6.2.0 betas did not have the fixes when the release shipped.

Can someone create an account on my Joomla site with registration turned off?

Before 5.4.9 and 6.1.4, yes. CVE-2026-90907 let an anonymous visitor post to the profile save task and create a user in the Guest group with a password of their choosing, even with Allow User Registration set to No. On a default permission setup that account cannot log in, but it exists, it can take an email address or username, and user plugins run for it.

Does the MFA bypass mean my second factor was useless?

No. CVE-2026-92227 needs the attacker to already know the password. With it, they could tick Remember Me on the front-end login, walk away from the MFA prompt, and come back later logged in by cookie with MFA skipped. It affects front-end logins only, because the administrator login has no Remember Me.

Can I update straight from Joomla 4 to 6.1.4?

No. Joomla 5.4.9 needs 4.4 as the starting point, and 6.1.4 needs 5.4. A site on 4.3 or earlier goes to 4.4, then 5.4.9, then 6.1.4 if you want Joomla 6.

Did these updates fix the Template Manager bug from 5.4.8?

Yes. The fix for the Snooping out of bounds error that 5.4.8 and 6.1.3 introduced is in both releases, so template overrides and new template folders work again after the update.

Does mySites.guru flag sites that still need this update?

Yes. The Joomla version check in the mySites.guru audit flags every connected site behind the latest release in its branch, and the bulk upgrade tool updates the selected sites in one pass.

AI MODIFIED

Written and edited by a human, with AI assistance. [Our approach to AI](#)

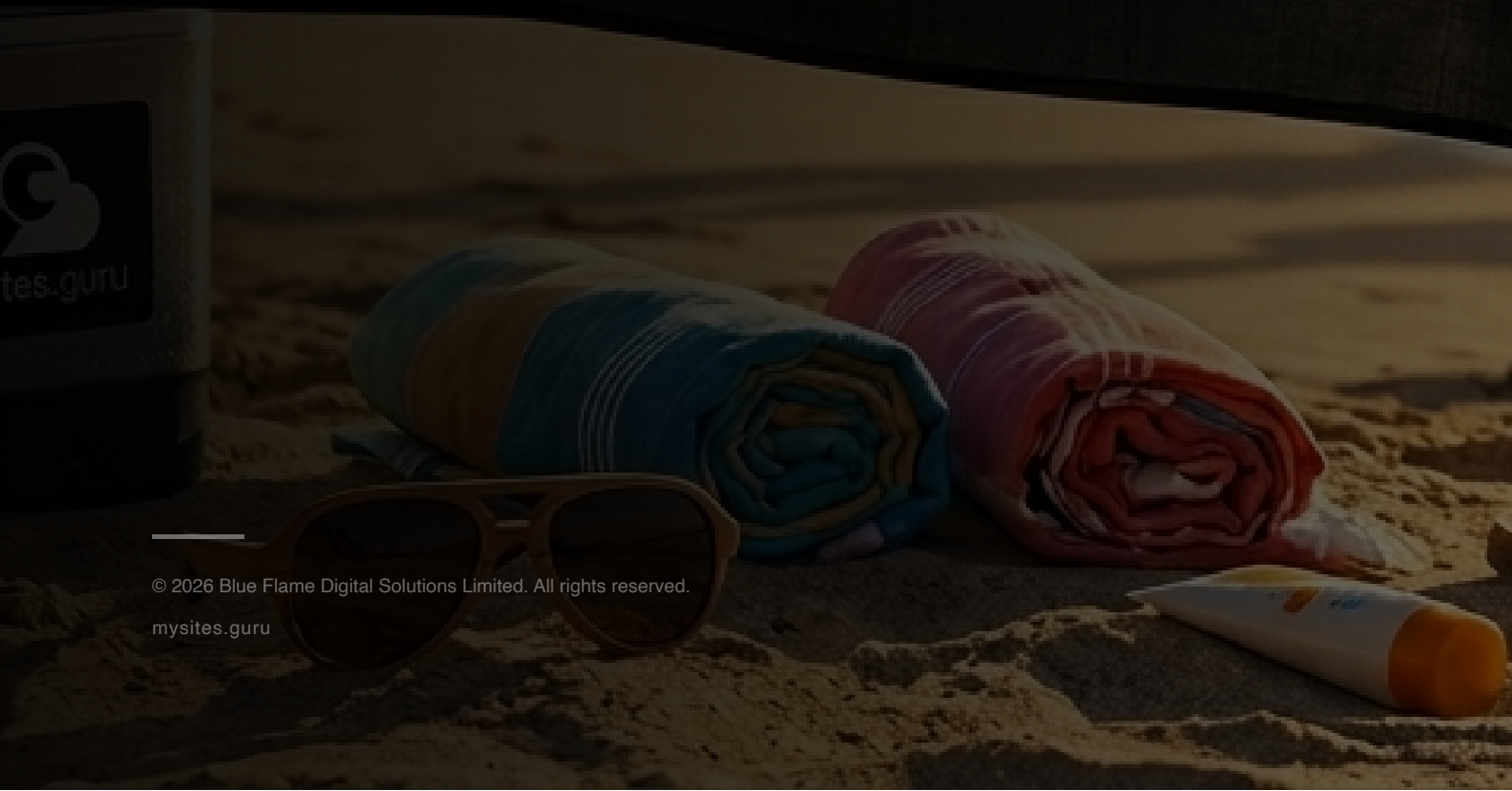
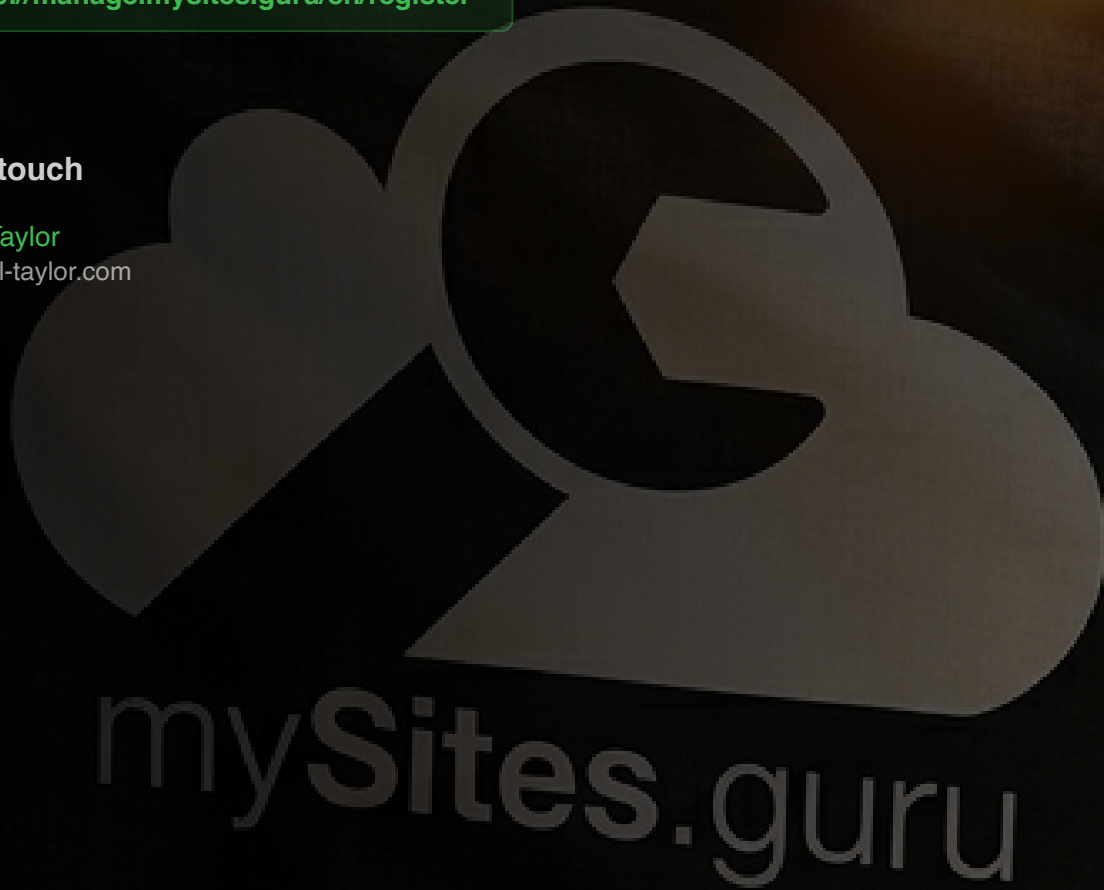
Get Your Free Site Audit

See how your WordPress and Joomla sites measure up.
No credit card required.

<https://manage.mysites.guru/en/register>

Get in touch

Phil E. Taylor
phil@phil-taylor.com



© 2026 Blue Flame Digital Solutions Limited. All rights reserved.

mysites.guru